Context

Jamcracker values its computing and network resources. As a system user of Jamcracker, you will have access to company resources that are sensitive. Strongly associated with the privilege of system access also comes a responsibility to conduct oneself in a manner deemed appropriate by Jamcracker.

Definitions

Anti-Virus Software: Software, designed to scan, detect and destroy any computer viruses contained within files, with the intent to prevent proliferation of the virus.

Audit trail: A record of events and transactions that provide evidence of system access and system processing, or attempts to gain system access or to perform system processing. Audit trails are typically captured and presented in chronological order.

Authentication: The process of determining whether a person, workstation, system, or procedure is eligible to access specific information, or to perform certain operations. Password validation, for example, is a form of authentication. Authentication may also be a measure meant to validate a transmission or message and the authority of the originator.

Backup: the process of copying data and software files to another media.

Password: A secret set of characters that, in conjunction with a public user ID, form a unique identifier representing a particular user.

User: All persons (employees or contractors) authorised to use Jamcracker resources to access a computer, the internal network and the Internet. This also includes anyone with access to e-mail, since e-mail enables the transmission of information across the Internet.

User ID: A string of characters that uniquely identifies a user to a computer system. User IDs are generally public knowledge. Under Jamcracker security standards, user IDs must be associated with a secret password. See also *Password*.

Virus: A program inserted into a computer system with the intent of committing mischievous or malicious damage. Viruses are capable of replicating themselves and of attaching themselves to (infecting) other programs or to the boot sector of diskettes, hard disks, or other storage media. Viruses are transmitted when an infected program runs on an uninfected system or an infected diskette is used by an uninfected system.

Virus scanner: A special type of software that detects either specific viruses or virus activity.

Individual Privilege

Every user will be issued a user ID and password that will allow access to his computer and to the network resources associated with his function. Therefore, the following must be agreed upon by the user:

1. This access can only be used to carry business approved by and related to Jamcracker.
2. Each user is assigned a folder located on shared corporate servers where data files can be stored for convenience.
3. An electronic mail (e-mail) account is issued to each user for the convenience of carrying activities related to Jamcracker. Occasionally, this e-mail account may be used for personal reasons, where used in a way as not to affect Jamcracker's reputation.
4. The Internet access is also granted and its use is driven by business needs.

Individual Responsibilities

The user of any computer system or any network is the first line of defense against misuse and against accidental loss of data. Therefore, every user must follow a strict set of guidelines aimed at protecting his interests and his colleague's here at Jamcracker. These guidelines are:

1. Read, understand and sign the **System User Security Policy Agreement**
2. Never share your user ID with anyone or leave the account open or unattended
3. Keep all user ID and passwords confidential and not accessible to others.
4. Infiltrating computer systems and/or damaging software components is prohibited.
5. Respect the rights and properties of others. Do not improperly access, misappropriate or misuse the files, data, or information of others.

6. Illegal activity is prohibited.
7. Illegal installation of copyrighted software or files is prohibited.
8. Excessive browsing and/or file transfers across the Internet for personal reasons is not allowed
9. Unattended computers must be logged off or protected in such a way as to protect the computer and network from unauthorized access.
10. Any observations of suspicious activity must be reported. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files

Jamcracker's Privileges

As for any corporation, Jamcracker is bound to many obligations in regard to the internal use of its computing and network resources. As such, Jamcracker must ensure that the resources are being used to their optimum. To that extent, Jamcracker may perform the following tasks, without being limited to these:

1. Inspect network traffic that is being sent and received from the user's workstation, both internally or through the Internet connection.
2. Access to any piece of information stored on Jamcracker's computer resources, including e-mail sent or received through Jamcracker corporate e-mail system.
3. Modify Internet access rules and privileges without giving a prior notice.
4. Re-assign a user ID.
5. Assign any IP address deemed reasonable to any computing resources.
6. Restrict access to files and programs located on the user's workstation.
7. Inspect at any time, which software packages are installed on each user's workstation
8. Maintain an audit trail of all network accesses for any purposes deemed necessary.
9. Audit the password strength of all corporate users on any platform.

Jamcracker's Responsibilities

As a commitment to the maximum business efficiency, and to all users of the corporate environment, Jamcracker commits itself to the following:

1. Maintain the local area network in reasonable working order. This includes taking appropriate measure to ensure availability as well as confidentiality and integrity.
2. Back up of all data files located on corporate servers
3. Initiate a corporate anti-virus action plan.
4. Update the virus signature definition files and distribute them regularly.
5. Provide every user with technical support for issues related to Jamcracker platform

Procedures and Sanctions

As stated in the Corporate IT Security Policy, the inappropriate use of Jamcracker's systems, accounts and resources, the unauthorized use of another person's computer account, and providing false or misleading information for the purpose of obtaining access to computer systems or modifying data, are prohibited and will be subject to the sanctions listed below. Any other violations of any provision of this policy may also result in:

- limitation on a user's access to some or all systems,
- the initiation of legal action by Jamcracker, including, but not limited to, criminal prosecution under appropriate state and federal laws,
- the requirement of the violator to provide restitution for any improper use of service, and
- disciplinary action up to and including termination.